REMARKS

The Office Action of December 8, 2003 has been carefully reviewed together with the references cited therein. In view of the claim amendments set forth above and the following remarks, the application is in condition for allowance.

Claims 1-16 were originally filed in this application, with claims 1, 9, 12, and 15 in independent form. With the foregoing amendments, claims 1-6, 8, 9, 11, 12 and 14-16 are pending. Claims 7, 10 and 13 are canceled.

The Office Action rejects claims 1-16 as originally filed for several reasons.

1. Claims 5, 9-11, 12-14 are rejected under 35 U.S.C. § 112, second paragraph, as indefinite.
2. Claims 9-14 are rejected under 35 U.S.C. § 101 as allegedly being directed to an inoperative invention and, therefore, lacking utility.
3. Claim 15 is rejected under 35 U.S.C. § 102(e) as being anticipated by Wood et al. (US Patent 6,609,198).
4. Claims 1, 2, 4-8 and 15 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Bodnar (U.S. Patent 6,061,790) in view of Wood et al.
5. Claims 3 and 16 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Bodnar and Wood et al. and further in view of Swift et al. (U.S. Patent 6,337,691).

THE SECTION 112 REJECTIONS

Turning first to the Section 112 rejection of claim 5, the Office Action considers the phrase "*a method under the hypertext transport protocol*" to be vague and indefinite. In response, applicant has amended the claim to change that phrase to "*a method defined in the Hypertext Transfer Protocol* (HTTP)." It is well known that the Hypertext Transfer Protocol (HTTP) is a communications protocol widely used to connect to servers on the World-Wide Web on the Internet

or on other networks. As shown in the document entitled "RFC 2068: Hypertext Transfer Protocol – HTTP/1.1," which is included in an Information Disclosure Statement submitted with this Amendment, the HTTP defines a plurality of methods (see Section 9). Thus, this amendment to claim 5 overcomes the Section 112 rejection.

As to the section 112 rejection of claims 9-11, the Office Action considers the clause "*authentication request data ... prompt a server not recognizing the authentication request data to respond ...*" to be confusing. To address this rejection, applicant has amended claim 9 to recite "*authentication request data ... cause a server not recognizing the authentication request data to respond ...*".

As for the Section 112 rejection of claim 11 concerning the phrases "... *data represent a method*" and the phrase "*a method under the hypertext transport protocol,*" applicant has amended claim 11 to recite "... *data identify a method defined in the Hypertext Transfer Protocol* (HTTP)". This amendment overcomes the rejection for the same reason provided above in connection with claim 5.

As for the Section 112 rejection of claims 12-14, the Office Action asserts that the phrase "*said data*" in claim 12 lacks antecedent basis. Applicant has changed "*said data*" to "*said authentication request data.*" The Office Action also asserts that the clause "*authentication request data ... prompt a server not recognizing the authentication request data to respond ...*" is confusing. Although applicant disagrees, in order to expedite prosecution the word "*prompt*" in the clause has been changed to "*cause*" in the same way claim 9 is amended as discussed above.

Finally, as to the Section 112 rejection of claim 14, the Office Action complains that the phrase "... *data represent an operation*" does not make sense since data cannot be an operation. In response, applicant has amended claim 14 to recite that the data "*identify*" an operation.

THE SECTION 101 REJECTION

Turning next to the Section 101 rejection, the Office Action rejects claims 9-14 for the allegedly describing an inoperative invention. The Office Action asserts that because the claims require the server not recognize a request, the claimed invention therefore has no utility, reasoning that the server cannot carry out the requested task without being able to recognize the request. The Office Action has missed the point of the claimed invention. The authentication request data in the network connection request by the client is intended for testing the server to see whether the server supports client-forced authentication. If the server recognizes the authentication request, it responds in a first way, and if the server does not recognize the authentication request, it responses in a second way. Based on the response from the server, the client can tell whether the server has recognized its authentication request, and can determine how to proceed. Thus, the utility of the claimed invention is the client's ability to tell from the server's response whether the server supports client-forced authentication, rather than guaranteeing that the server will carry out the requested task, namely establishing an authenticated HTTP connection with the client. With this proper understanding of the claimed invention based on the plain meaning of the specification, the Section 101 rejection must be withdrawn.

THE PRIOR ART REJECTION

In this amendment, the claims have been amended to emphasize that the context of the invention, which is establishing a network connection under the Hypertext Transfer Protocol (HTTP) between a client and a server. Thus, a request by a client that carries authentication request data and a response by a server are formatted as HTTP packets.

In rejecting the claims as originally presented, the Office Action relies on Bodnar, Wood et al., and Swift et al. None of these references, however, addresses the problem of forming an authenticated network connection under the HTTP between a client and a server. More specifically, even though these three references describe certain implementations of client-

authentication schemes in their respective given contexts, they do not address the problem of enabling a HTTP client to initiate the formation of an authenticated network connection under the Hypertext Transfer Protocol with a HTTP server.

Bodnar is directed to a system that allows authentication of a user even thought the network client machine used by the user does not know the authentication credentials of the user. *See*, Bodnar, col. 3, lines 34-41.

Wood et al. is directed to a log-on service that allows a user or application to provide additional credentials for authentication at a higher trust level without loss of session continuity. *See*, Wood et al., col. 16, lines 18-56.

Swift et al. discloses a system that uses a challenge-response authentication protocol for datagram-based remote procedure calls. *See*, Swift et al., col. 3, lines 29-35.

None of these three references teaches or suggests the solution to the connection problem provided by the claimed invention. Specifically, the cited references do not teach or suggest the inclusion of data requesting for an authenticated connection in the client's HTTP connection request to the server, or the client's action depending on whether the server's response indicates that the server recognizes the authentication request. For at least these reasons, the claims as amended are allowable over these cited references.

By way of background and to facilitate a better understanding of the applicant's invention and how it differs from the prior art of record, a short summary of the claimed invention follows. The claimed invention enables a client wanting to form a network connection with a server under the Hypertext Transfer Protocol (HTTP) to force the server to establish an authenticated connection. As explained in the Background section of the specification, conventionally under the HTTP protocol only the HTTP server is given the ability to enforce the client authentication. *See*, Specification p. 2, lines 2-9; HTTP/1.0; HTTP/1.1. The invention provides a way for a HTTP client to request a HTTP server to establish an authenticated HTTP connection. This

approach addresses the problem posed by some older HTTP servers that may not support the client-forced authentication.

Specifically, the client includes an authentication request in the connection request packet under the HTTP to the server for initiating the network connection. If the HTTP server recognizes the client's authentication request data and supports the client-forced authentication, it responds in a way indicating it supports client-forced authentication. On the other hand, if the HTTP server is an older server that does not recognize the client's authentication request data, it responds in another well-defined way, such as sending an error message defined in HTTP.

In keeping with the invention, based on the HTTP server's response to the client, the client is able to tell whether the server supports client-forced authentication, and preferably whether the HTTP connection is already authenticated. If the response from the HTTP server indicates it supports the client-forced authentication and that the HTTP connection is not yet authenticated, the client may send its credentials to the server for authentication. On the other hand, if the response of the HTTP server indicates the server does not support client-forced authentication, the client may decide to communicate further with the server over a non-authenticated HTTP connection.

Conclusion:

This application is considered to be in condition for allowance, and the examiner is respectfully requested to pass this application to issue. If, in the opinion of the examiner, a telephone conference would expedite the prosecution of the subject application, the examiner is invited to call the undersigned attorney.

Respectfully submitted,

John B. Conklin, Reg. No. 30,369
One of the Attorneys for Applicant
LEYDIG, VOIT & MAYER, LTD.
Two Prudential Plaza, Suite 4900
180 North Stetson
Chicago, Illinois 60601-6780
(312) 616-5600 (telephone)
(312) 616-5700 (facsimile)

Date: May 6, 2004